数理解析研究所講究録
第 1593 巻 2008 年 93-98

Simple 3-designs on $q+2$ points constructed from $PSL(2,q)$, $q \equiv 3 \pmod 4$

Izumi Miyamoto
University of Yamanashi

Let $X=\{0,1,2,\cdots,n\}$. Let B be a set of k-point subsets of X. Here B may be a multi-set. Then (X,B) is called a t-$(n+1,k,\lambda)$ design if every t-point subset of X is contained exactly λ elements of B. An element of B is called a block. A design (X,B) is called simple, if there are no repeated blocks in B.

Let G be a permutation group on X.

t-Transitive and t-Homogeneous:

Let $x_1, x_2, \cdots, x_t$ and $y_1, y_2, \cdots, y_t$ be a couple of t points of X.

$$G \text{ is } t\text{-transitive.}$$
$$\Updownarrow$$
$$\exists g \in G \text{ such that } x_1^g = y_1,\ x_2^g = y_2,\ \cdots,\ x_t^g = y_t.$$
$$G \text{ is } t\text{-homogeneous.}$$
$$\Updownarrow$$
$$\exists g \in G \text{ such that } \{x_1^g, x_2^g, \cdots, x_t^g\} = \{y_1, y_2, \cdots, y_t\}.$$

Examples

$G=PGL(2,q)$, projective general linear group over a field of q elements.

$\Rightarrow$ G is 3-transitive.

$G=PSL(2,q)$, projective special linear group over a field of q elements, q odd.

$\Rightarrow$ G is 2-transitive.

G is 3-homogeneous if $q=3$ mod 4.

Action of G in k-point subsets:

Let $b=\{x_1,x_2,\cdots,x_k\}$, a k-point subset of X. We denote $\{x_1^g,x_2^g,\cdots,x_k^g\}=\{x_1,x_2,\cdots,x_k\}^g$.

Let $B = \{b^g | g \in G\}$, the *orbit* of G containing b.

$$G \text{ is } t\text{-homogeneous.} \Longrightarrow (X, B) \text{ is a simple } t\text{-design.}$$

Here we assume G is t-homogeneous on $\{1, 2, \cdots, n\} = X \backslash \{0\}$ and G leaves the point 0 fixed. We want to choose orbits B_0, B_1, B_1' of G on $(k+1)$-point subsets so that

$b_0 \in B_0 \Longrightarrow 0 \in b_0$

$b_1 \in B_1 \cup B_1' \Longrightarrow 0 \notin b_1$

$c_0 B_0 \cup c_1 B_1 \cup c_1' B_1'$ becomes the blocks of a t-design,

where $c_j B_j$ means every subset in B_j is repeated c_j times. Here we quote a theorem which will be shown in [4]

Theorem 1 *Let* $B = c_0 B_0 \cup c_1 B_1 \cup c_1' B_1'$, *where* c_0, c_1 *and* c_1' *satisfy*

$$\frac{(n-k)c_0}{(k+1)g_0} = \frac{c_1}{g_1} + \frac{c_1'}{g_1'}.$$

Then (X, B) *is a* t-$(n+1, k+1, \lambda)$ *design with*

$$\lambda = \frac{c_0 g \binom{k}{t-1}}{g_0 \binom{n}{t-1}}.$$

In particular, if $c_1' = 0$, *then* $B = c_0 B_0 \cup c_1 B_1$ *and the above condition becomes*

$$\frac{c_1}{c_0} = \frac{g_1(n-k)}{g_0(k+1)}.$$

Examples

$G = PSL(2, q)$ or $PGL(2, q)$ acting on projective line $\mathbf{P} = \{1, 2, \cdots, q+1\}$. If $G = PSL(2, q)$, we assume that $q = 3 \bmod 4$ so that G is 3-homogeneous. $G_{1,2}$ = stabilizer of points 1 and 2 in G We assume $q = 1 \bmod 6$, which implies $3 | q-1$. So $G_{1,2}$ has subgroups of order 3 and $\frac{1}{2}(q-1)$ having $\frac{1}{3}(q-1)$ orbits of length 3 and of order $\frac{1}{2}(q-1)$ having two orbits of length $\frac{1}{2}(q-1)$ respectively. We use some of these orbits to construct blocks. Set $b_0 = \bigcup \frac{1}{6}(q-7)$ orbits of length 3 $\bigcup \{0, 1, 2\}$ $b_1 = \bigcup \frac{1}{6}(q-1)$ orbits of length 3 b_1' = a orbit of length $\frac{1}{2}(q-1)$ Then the block size is $k+1 = \frac{1}{2}(q-1)$. The orders of the stabilizers of the blocks b_0, b_1, b_1' should be $g_0 = 3c_0$, $g_1 = 3c_1$, $g_1' = \frac{c_1'}{2}(q-1)$ Set $B = c_0B_0 \cup c_1B_1 \cup c_1'B_1'$. Then we have

$$\frac{(n-k)c_0}{(k+1)g_0} = \frac{q+1-\frac{1}{2}(q-3)}{\frac{1}{2}(q-1)\times 3} = \frac{q+5}{3(q-1)}$$

$$\frac{c_1}{g_1} + \frac{c_1'}{g_1'} = \frac{1}{3} + \frac{2}{q-1} = \frac{q+5}{3(q-1)}$$

$|G| = \frac{1}{m}(q+1)q(q-1)$, where $m = 2$ or 1 according as $G = PSL(2,q)$ or $PGL(2,q)$.

$$\lambda = \frac{(q-1)(q-3)(q-5)}{12m}$$

Theorem 2 [3] $(\mathbf{P}\cup\{0\}, B)$ *is a* 3-$(q+2, \frac{1}{2}(q-1), \frac{1}{12m}(q-1)(q-3)(q-5))$ *design.*

G is as above. Similarly we chose 3 subsets of $\mathbf{P}\cup\{0\}$ of size $\frac{1}{2}(q+1)$ so that the stabilizers are of order $g_0 = c_0$, $g_1 = c_1$, $g_1' = \frac{c_1'}{2}(q+1)$

Theorem 3 $(\mathbf{P}\cup\{0\}, B)$ *is a* 3-$(q+2, \frac{1}{2}(q+1), \frac{1}{4m}(q-1)^2(q-3))$ *design.*

Simple designs

Let $G = PSL(2,q)$, $q \equiv 3 \pmod 4$. From Theorem 2, if there exist b_0, b_1 and b_1' of size $\frac{1}{2}(q-1)$ such that

$$|G_{b_0\setminus\{0\}}| = 3, \quad |G_{b_1}| = 3, \quad |G_{b_1'}| = \frac{1}{2}(q-1),$$

then we have a simple 3-design.

Similarly from Theorem 3, if there exist b_0, b_1 and b_1' of size $\frac{1}{2}(q+1)$ such that

$$|G_{b_0\setminus\{0\}}| = 1, \quad |G_{b_1}| = 1, \quad |G_{b_1'}| = \frac{1}{2}(q+1),$$

then we have a simple 3-design.

The number of k-subsets with stabilizer group precisely H for a subgroup H of $PSL(2,q)$ is determined in [2] if $k \not\equiv 0, 1 \pmod p$, where q is a power of a prime p and $q \equiv 3 \bmod 4$. The number is denoted by $g_k(H)$. A cyclic group of order l, a dihedral group of order $2l$, an alternating and a symmetric group of degree 4 will be denoted by C_l, D_{2l}, A_4 and S_4 respectively. A_5 denotes a alternating group of degree 5.

For Theorem 2 it suffices to show that

$$g_{\frac{1}{2}(q-3)}(C_3) > 0, \quad g_{\frac{1}{2}(q-1)}(C_3) > 0 \text{ and } g_{\frac{1}{2}(q-1)}(C_{\frac{1}{2}(q-1)}) > 0$$

For Theorem 3,

$$g_{\frac{1}{2}(q-1)}(C_1) > 0 \quad g_{\frac{1}{2}(q+1)}(C_1) > 0 \quad g_{\frac{1}{2}(q+1)}(C_{\frac{1}{2}(q+1)}) > 0$$

Let $f_k(H)$ denotes the number of k-subsets left invariant by a subgroup H and let $\mu(l)$ denotes the Möbius function. In Table 2 in [2] $f_k(H)$ are obtained for various subgroups H of $PSL(2,q)$. In Theorem 24, 25 and 26 in [2] $g_k(C_1)$, $g_k(C_2)$ and $g_k(C_3)$ are expressed with $f_k(H)$. So we have the following.

$$\begin{aligned} g_{\frac{1}{2}(q-3)}(C_3) &= -\tfrac{q-1}{3} f_{\frac{1}{2}(q-3)}(A_4) + f_{\frac{1}{2}(q-3)}(C_3) - \tfrac{q-1}{6} f_{\frac{1}{2}(q-3)}(D_6) \\ g_{\frac{1}{2}(q-1)}(C_3) &= \sum_{l \mid \frac{1}{6}(q-1)} \mu(l) f_{\frac{1}{2}(q-1)}(C_{3l}), \end{aligned}$$

where p_1 is the smallest prime factor of $\frac{1}{6}(q-1)$.

$$g_{\frac{1}{2}(q-1)}(C_1) = f_{\frac{1}{2}(q-1)}(C_1) + \sum_{l>1, l \mid \frac{1}{2}(q-1)} \tfrac{q(q+1)}{2} \mu(l) f_{\frac{1}{2}(q-1)}(C_l)$$

$$\begin{aligned} g_{\frac{1}{2}(q+1)}(C_1) &= f_{\frac{1}{2}(q+1)}(C_1) \\ &+ \tfrac{q(q^2-1)}{12}(2f_{\frac{1}{2}(q+1)}(A_4) - 6f_{\frac{1}{2}(q+1)}(S_4) - 12f_{\frac{1}{2}(q+1)}(A_5) + f_{\frac{1}{2}(q+1)}(D_4)) \\ &+ \sum_{l>1, l \mid (q\pm1)/2} \tfrac{q(q\mp1)}{2} \mu(l) f_{\frac{1}{2}(q+1)}(C_l) - \tfrac{q(q^2-1)}{4} \textstyle\sum_{l>2, l \mid (q+1)/2} \mu(l) f_{\frac{1}{2}(q+1)}(D_{2l}) \end{aligned}$$

In order to see $g_k(H) > 0$, we use the following lemmas.

Lemma 4 *Let m and t be integers greater than 1. Assume t divides m. Then*

$$(1) \quad \binom{2m}{m} > 2^{m-\frac{m}{t}} \left(\tfrac{t+1}{2}\right)^{\frac{m}{t}} \binom{2m/t}{m/t}$$

$$(2) \quad \binom{4m+2}{2m} > 2^{2m} \binom{2m+1}{m} \text{ and } \binom{4m}{2m} > 2^{2m-1} \binom{2m}{m}$$

Lemma 5 *Let p_1, p_2, $\cdots$, p_r be the prime factors of m. Then*

$$-\sum_{i=1}^{r}\binom{2m/p_i}{m/p_i} \le \sum_{l>1,l|m}\mu(l)\binom{2m/l}{m/l} < -\tfrac{7}{8}\sum_{i=1}^{r}\binom{2m/p_i}{m/p_i}$$

Lemma 6

$$\sum_{l>1,l|m}\mu(l)\binom{2m/l}{m/l} > -\tfrac{3}{2}\binom{2m/p_1}{m/p_1},$$

where p_1 is the smallest prime factor of m.

The proofs will be shown in [4]. Then we will have the following simple designs.

Theorem 7 *If $q \equiv 7 \bmod 12$ and $q > 19$, then there exists a simple 3-$(q+2, \frac{1}{2}(q-1), \frac{1}{24}(q-1)(q-3)(q-5))$ design $(\mathbf{P}\cup\{0\}, B)$, where B consists of three orbits B_0, B_1 and B_1' of $PSL(2,q)$ acting on the $\frac{1}{2}(q-1)$-point subsets of $\mathbf{P}\cup\{0\}$ such that $0 \in b_0$, $0 \notin b_1$ and $0 \notin b_1'$ for $b_0 \in B_0$, $b_1 \in B_1$ and $b_1' \in B_1'$ and that the stabilizers of them are C_3, C_3 and $C_{\frac{1}{2}(q-1)}$ respectively.*

Theorem 8 *If $q \equiv 3 \bmod 4$ and $q \ge 19$, then there exists a simple 3-$(q+2, \frac{1}{2}(q+1), \frac{1}{8}(q-1)^2(q-3))$ design $(\mathbf{P}\cup\{0\}, B)$, where B consists of three orbits B_0, B_1 and B_1' of $PSL(2,q)$ acting on the $\frac{1}{2}(q+1)$-point subsets of $\mathbf{P}\cup\{0\}$ such that $0 \in b_0$, $0 \notin b_1$ and $0 \notin b_1'$ for $b_0 \in B_0$, $b_1 \in B_1$ and $b_1' \in B_1'$ and that the stabilizers of them are C_1, C_1 and $C_{\frac{1}{2}(q+1)}$ respectively.*

We note that it is a popular method to construct designs using some orbits of permutation groups, if the number of the points is fixed. For instance, readers may refer to [1]. We also note that $g_{\frac{1}{2}(q-3)}(C_3) = 0$ if $q = 19$ below. So we will construct a simple design in the following section from $PSL(2,19)$ by a similar method shown in Theorem 1.

$$\begin{aligned}
g_{\frac{1}{2}(q-3)}(C_3) &= -\tfrac{q-1}{3}f_{\frac{1}{2}(q-3)}(A_4) + f_{\frac{1}{2}(q-3)}(C_3) - \tfrac{q-1}{6}f_{\frac{1}{2}(q-3)}(D_6)\\
&= -\tfrac{q-1}{3}\binom{(q-7)/12}{(q-19)/24} + \binom{(q-1)/3}{(q-7)/6} - \tfrac{q-1}{6}\binom{(q-1)/6}{(q-7)/12}\\
&= -6\binom{1}{0} + \binom{6}{2} - 3\binom{3}{1} = -6 + 15 - 9 = 0
\end{aligned}$$

Experiments

$G = PSL(2, 19)$ =`PrimitiveGroup`$(20, 1)$ of order 3420. G is 3-homogeneous on $\boldsymbol{P} = \{1, 2, \cdots, 20\}$. Here we consider the additional point 21. So $X = \boldsymbol{P} \cup \{21\}$. We take the following 4 9-point subsets of X, $\{1, 2, 3, 4, 9, 10, 15, 16, 21\}$, $\{1, 2, 3, 6, 9, 12, 15, 18, 21\}$, $\{3, 4, 5, 9, 10, 11, 15, 16, 17\}$ and $\{3, 5, 7, 9, 11, 13, 15, 17, 19\}$. The stabilizers of these subsets are of order 6, 6, 3 and 9, respectively. Let B be the union of the 4 orbits of G acting on the 9-point subsets of X containing these 4 subsets. Then B becomes the block set of a 3-$(21, 9, 168)$ design.

$G = PGL(2, 25)$ =`PrimitiveGroup`$(26, 2)$. We can choose the blocks of size $\frac{1}{2}(q-1) = 12$ so that the stabilizers are of order 6, 6, 24. So by Theorem 2 $c_0 = c_1 = c_1' = 2$ and $B = 2B_0 \cup 2B_1 \cup 2B_1'$. So, if we set $B = B_0 \cup B_1 \cup B_1'$, we have a simple 3-(27,12,440) design.

$G = PGL(2, 25)$ =`PrimitiveGroup`$(26, 2)$. We can choose the blocks of size $\frac{1}{2}(q+1) = 13$ so that the stabilizers are of order 2, 2 and 26. So by Theorem 3 $c_0 = c_1 = c_1' = 2$. We have a simple 3-(27,13,1584) design if we set $B = B_0 \cup B_1 \cup B_1'$.

We used GAP system in our experiments.

References

[1] A. Betten, E. Haberberger, R. Laue, A. Wassermann, DISCRETA - a program to construct t-designs with prescribed automorphism group. http://www.mathe2.uni-bayreuth.de/discreta/

[2] P. J. Cameron, H.R.Maimani, G.R.Omidi and B. ayfeh-Rezaie, 3-Designs from PSL$(2, q)$. *Discrete Math.*, 306 (2006) 3063–3073.

[3] I. Miyamoto, A construction of designs from $PSL(2, q)$ and $PGL(2, q)$, $q \equiv 1 \pmod 6$, on $q + 2$ points. *to appear in Algorithmic Algebraic Combinatorics and Gröbner Bases, edited by G.Jones, A. Jurisic, M. Muzychuk and I. Ponomarenko* Springer.

[4] I. Miyamoto, A construction of designs on $n + 1$ points from multiply homogeneous permutation groups of degree n. in preparation.